Title:	Information Technology Governance & Cybersecurity Policy and Procedures
Approved:	December 7, 2022
Approved by:	Dean's Executive Committee
Audience:	Faculty-Wide
Purpose:	Enable secure and compliant operation of Faculty of Medicine technology
Contact:	Digital Solutions

Background & Purpose

The University of British Columbia (UBC) Faculty of Medicine (FoM) education and research programs operate in a complex distributed environment across British Columbia. Information technology is a crucial enabler for our educators, scientists, learners, and staff. The increasing use of technology comes with risks which must be managed to avoid compromises of privacy, intellectual property, and loss of public and partner trust.

All IT operations within the FoM are subject to UBC Policy SC14 – Acceptable Use and Security of UBC Electronic Information and UBC Information Security Standards (ISS), as well as other policies related to procurement of IT related goods and services. The purpose of UBC policy SC14 and the ISS is to reduce risk to the Faculty and the Institution – reputational risk from the disclosure of personal or sensitive data, operational risk from downtime of crucial systems due to security compromise, and financial risk from ransomware or intellectual property theft.

In addition to the requirements of the UBC policies, this document defines additional requirements within the FoM to improve the safety and security of our IT systems, and lays out procedures that are expected to be followed in each unit.
The purpose of this document is to:

1. Provide clarity on the application of UBC policies in all FoM units and environments, particularly locations outside of the UBCV main campus;
2. Define reporting requirements of all staff and contractors performing IT-related duties;
3. Clarify procedures to ensure compliance with UBC IT related policies and standards;
4. Promote efficient and effective use of technology resources within the FoM.

Scope

The Faculty of Medicine will implement and maintain a centrally managed compliance monitoring program to support units in achieving security compliance. This applies to all FoM departments, schools, centers & institutes, administrative units, academic programs, and research projects undertaken by faculty, students, and trainees where UBC is the host institution. This document contains both policy elements and procedures that outline how the FoM will remain compliant with the relevant UBC policies listed above.

Policy

1. Staff managing or overseeing University & Faculty IT assets and operations must have a dotted-line or solid-line reporting relationship to FoM Deputy CIO Medicine (DCIO-M) or their delegate within Digital Solutions (DS).
2. External IT vendor contracts within the FoM must be reviewed and approved via the FoM Office of the Deputy CIO Medicine (DCIO-M Office), with reporting requirements equivalent to that of staff.
3. Audio and video technology used for teaching distributed education programs must meet the A/V standards set by FoM Digital Solutions (DS) collaboration office. Any exceptions must be approved by the DCIO-M Office.
4. To ensure the best use of public resources, the Faculty expects units to avoid duplication of IT and data services provided by UBC IT or FoM Digital Solutions the DCIO-M Office.
5. Declaration of compliance with institutional IT policies and security standards must be documented for all units within FoM on an annual basis.
6. In the event of security compromise of locally managed IT systems found to be non-compliant with related policies and standards, the respective unit will need to contribute to the costs associated with incident mitigation, including but not limited to investigation, forensics, and any other costs associated with the breach. Costs related to centrally managed systems will be met by the supporting organization.
7. A unit found non-compliant with these measures or the procedures listed below will be asked to prepare a report outlining their risk mitigation approaches and plans to become compliant. That may be presented to the Dean or FoM IT Committee, depending on the risk. If the unit does not meet the requirements to become compliant, they will be denied access to UBC IT network and information systems.

Procedures – All

The following procedures are applicable to all Faculty of Medicine departments, schools, programs, and research units.

1. **IT Governance**
    1. Staff and contractors managing or overseeing University & Faculty IT assets and operations are accountable to the FoM DCIO-M office, for maintaining those assets in line with UBC's policies and complying with Governance. This must be reflected in job descriptions, position profiles or contracts, whether hired through UBC or a partner institution. For clarity, the DCIO-M office does not oversee individual performance, compensation, or other employment terms for staff employed by a third party, including Partner Institutions.
    2. Faculty of Medicine units should avoid duplication of IT and data services provided by UBC IT, FoM Digital Solutions (DS), or Partner Institution IT Teams. A business case for exception must be documented and approved by the dcio.medicine@ubc.ca
    3. Faculty of Medicine units making capital investment in information technology assets must follow UBC FM11 policy. IT projects with aggregate estimate value over five years of $75,000 must be approved/endorsed through FoM IT Committee (ITC). For IT projects over $75,000 please email dcio.medicine@ubc.ca

2. **Compliance, Monitoring, and Auditing**
    1. Faculty of Medicine units fully utilizing centrally provisioned IT services will not be required to declare compliance at an individual unit level. This will be done on behalf of the units by the FoM DCIO-M Office.
    2. Units must designate an individual who will be the point of contact for IT related communications and co-ordination of institutional awareness and training campaigns.
    3. Faculty, staff, researchers, student employees and contractors must complete Privacy and Information Security Fundamental 1 & 2 training as part of UBC required general courses.
    4. Faculty, staff, researchers, student employees and contractors who have a technical role must also complete Privacy & Information Security training for IT Professionals. https://srs.ubc.ca/training/privacy-information-security/
    5. All devices used for university business – whether they are owned by the University, by the user, or by a third party- need to be protected based on the UBC ISS U7 – Securing Computing and Mobile Storage Devices/Media. Devices used for university business but procured and managed through health authority

or partner institution IT organization and meeting equivalent UBC IT-related policies and standards are considered compliant and therefore exempted.

3. **Security Event and Incident Handling**
    1. Any suspicious incidents relating to the security of UBC electronic information and systems must be reported to security@ubc.ca and the UBC ISS U4 – Reporting Information Security Incidents standard must be followed.

4. **Vendor Contracts**
    1. New IT vendor contracts for goods and/or services must be reviewed by or established in consultation with the FoM DCIO-M.
    2. All contracts must follow the UBC University Counsel's Contracts and Signing process.
    3. External IT vendors contracts must include an undertaking to comply with this Policy and any relevant UBC policies and standards.
    4. Non-UBC employees – e.g., contractors, sub-contractors, or vendor employees - must sign a Security and Confidentiality Agreement (SACA) before being given access to personal or otherwise confidential/sensitive information held by UBC, they Refer to the University Counsel's webpage for details and sample SACA.
    5. Vendor employees are subject to training requirements per 2.3 and 2.4 above.

Procedures – Independent IT Function

The following procedures are applicable only to Faculty of Medicine departments, programs, and research units who have local or independently managed IT function (i.e. not managed by UBC IT, UVic or UNBC IT, FoM Digital Solutions or Health Authority IT unit).

1. **Compliance, Monitoring, and Auditing**
    1. With support from FoM Digital Solutions, the Administrative Heads of Units with independent or vendor managed IT environment must on an annual basis declare compliance with Institutional policies and standards (SC14 and the ISS), utilizing the PRISM Attestation form.
    2. Units must designate a technical contact who is responsible for ensuring compliance with UBC information security standards.

3. Units must use the central FoM asset register to maintain a list of critical electronic assets and the security classification of the information processed by or stored on that asset.
4. UBC and/or FoM Information Security staff must have access to perform security audits and scanning on any system in the FoM including all systems attached to UBC IT network.
5. Audits may need to be performed to investigate security incidents and/or to ensure conformance to the UBC security policies. Results of audits will remain confidential and are intended solely to provide information to help protect FoM data.
6. When requested, for the purposes of performing an audit, access will be provided to members of the UBC Information Security staff. This access may include:
    1. User and/or system level access to any computing or communications device.
    2. Access to department level firewall (read only) and firewall logs.
    3. Access to interactively monitor and log traffic on UBC IT networks.
    4. Permission for UBC IT scanning system to access and scan internal networks.
7. Users, devices, and IT networks found to be non-compliant with the UBC policy and security standards will be asked to provide a plan to become compliant. If they do not meet that plan, they will be denied access to the UBC IT network and information systems.

2. Security Event and Incident Handling

1. Units must designate a technical representative who will be responsible for coordinating with UBC and/or FoM Information Security staff to address any local issues in the event of potential compromise or exploit of UBC system or electronic information. This may include after-hours coverage.
2. When responding to a security incident, the UBC Information Security team may need the local team to secure and preserve electronic evidence for the purpose of incident investigation. Procedures are laid out in Securing and Preserving Electronic Evidence Guideline

Definitions

1. **IT Vendor Contract:** A contract involving the design, development, implementation, or operation of any UBC electronic information or systems through commercially provided products and services.
2. **Critical Electronic Assets:** These are UBC electronic information and systems which, in the event of a data breach or system failure, could have a negative impact on our mission, safety, finances, or reputation.
3. **UBC Electronic Information and Systems:** Includes UBC Electronic Information and UBC Systems.
4. **UBC Electronic Information:** Electronic information needed to conduct University Business.
5. **UBC Systems:** These are services, devices, and facilities that are owned, leased or provided by the University, and that are used to store, process or transmit electronic information. These include, but are not limited to:
    - 5.1. Computers and computer facilities;
    - 5.2. Computing hardware and equipment;
    - 5.3. Mobile computing devices such as laptop computers, smartphones, and tablet computers;
    - 5.4. Electronic storage media such as CDs, USB memory sticks, and portable hard drives;
    - 5.5. Communications gateways and networks; email systems;
    - 5.6. Telephone and other voice systems; and software.
6. **University Business:** Means activities in support of the administrative, academic, and research mandates of the University.
7. **Users:** These are faculty, staff, students, and any other individuals who use UBC Electronic Information and System.
8. **Partner Institutions:** Health Authority, collaborating post-secondary institutions or other such organizations who provide IT services to support university business activities.